REMARKS

The present amendment is submitted in response to the Final Office Action mailed November 14, 2007. Claims 1-13 remain in this application. Claims 1, 10, 11, 12, 22 and 23 are in independent form. In view of the amendments above and the remarks to follow, reconsideration and allowance of this application are respectfully requested.

Interview Summary

Applicants appreciate the courtesy granted to Applicant's attorney, Michael A. Scaturro (Reg. No. 51,356), during a telephonic interview conducted on Tuesday, January 8, 2008. During the interview, the underlying motivation for the invention was initially discussed. In particular, it was pointed out that the invention provides a reproducing apparatus, method and record carrier which provides a high degree against hacking, i.e., making it more difficult to make a player region code free. The invention allows, for example, a movie studio to control the timing of DVD releases by not allowing playback devices to play discs from any region.

In addition to providing a general overview, during the interview, certain distinguishing features between the invention and Kocher (the cited 102 reference) were discussed. These features include certain keys being stored on the record carrier (e.g., RCC, RK) which are not taught in Kocher. As a further point of distinction, these unique keys are pro-actively retrieved by the playback device, which is also not taught in

Kocher. While the Examiner generally agreed that the Kocher reference was overcome, he indicated that a further study of Kocher would be required.

35 U.S.C. §102(b)

Claims 1-3 and 9-13 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent 6,289,455 – Kocher et al – hereinafter Kocher.

Regarding original claim 1, the Office Action states Kocher teaches the elements of claim 1.

Applicants respectfully traverse the rejection under 102(b), however, Independent Claims 1, 11 and 12 have been amended herein to better define Applicant's invention over Kocher.

With respect to Claim 1, it now more clearly recites that the record carrier stores – (1) content in encrypted form, (2) a carrier region code (RCC) indicating in which region said content shall be allowed to be reproduced and (3) an encrypted region key (RK) for decrypting said content. Further, Claim 1 also now more clearly recites that the carrier stored content, RCC and RK keys are operated on by playback device apparatus comprising **(a) region code storage means (10)** for storing a device region code (RCD) for use by a region code check unit, **(b) a device key storage means (11)** for storing a device key (DK), said device key (DK) being different for all regions, **(c) a carrier region code reading means (12)** for reading said carrier region code (RCC)

from said record carrier (2), for use by said region code check unit **(d) a region code check unit (13)** for checking if said carrier region code (RCC) matches said device region code (RCD) to determine if said record carrier is allowed to be reproduced by said reproducing apparatus, **(e) a region key reading means (14)** for reading said encrypted region key (RK) from said record carrier (2) upon receiving an indication of a match between said device region code (RCD) and said carrier region code (RCC) from said region code check unit, **(f) a region key decryption means (16)** for decrypting said encrypted region key (RK) using said device key (DK) in case said carrier region code (RCC) matches said device region code (RCD), **(g) a content reading means (17)** for reading said encrypted content from said record carrier (2), and **(h) a content decryption means (18)** for decrypting said encrypted content using said decrypted region key.

With respect to Claim 1, it is respectfully submitted that Kocher does not teach or disclose at least the features recited above in claim 1, as amended. Specifically, as indicated above, claim 1 recites that the record carrier stores (1) content in encrypted form, (2) a carrier region code (RCC) indicating in which region said content shall be allowed to be reproduced and (3) an encrypted region key (RK) for decrypting said content.

In contrast, Kocher teaches that the playback device of Kocher **receives content** from a provider 200 who prepares it for distribution by compressing and encrypting the content, and adding control messages, such as KDMs and REMs (see Kocher at Col. 9,

lines 1-6). Therefore, Kocher does not store a carrier region code (RCC) or an encrypted region key (RK) with the encrypted content. Further, it is noted that Kocher receives content and **does retrieve content,** as taught by the invention.

As a further point of distinction, it is noted that the KDM and REM messages, which are transmitted along with the encrypted content in Kocher, serve a different purpose than the RCC and RK keys which are retrieved by the playback device of the invention. Specifically, Kocher teaches that to decode content, the KDM message is used by the playback device to derive one or more content decryption keys **stored in the CryptoFirewall's protected memory** (See Kocher at Col. 9, lines 42- 50). In contrast to the method of Kocher for accessing content, the invention retrieves an encrypted key from the record carrier and decrypt the key using a stored device key. That is, the content decryption key is not stored in the playback device, in contrast to Kocher. A method for accessing content is disclosed in Kocher at Cols. 11 and 12:

Accessing content: Before a user can access some content, the playback device must obtain the correct content decryption key (CDK) so that the content can be decrypted. FIG. 5 shows an exemplary method of the present invention for deriving CDKs **using rights keys stored in the CryptoFirewall's protected memory.** At step 500, the interface control processor (ICP) **receives a key derivation message (KDM)** from the playback device. At step 510, the ICP **uses the KDM to obtain a CDK generator value.** (The CDK generator is typically an encrypted form of the CDK and is part of the KDM.) The ICP then sends the CDK generator and an address in the protected memory corresponding to the appropriate rights key to the CryptoFirewall, which performs steps 520 through 560. (To assist with selecting the correct address, the ICP can use its nonvolatile memory to keep track of the rights keys and their locations. The KDM also can identify which rights key is appropriate for processing each CDK generator.) At step 520, the CryptoFirewall verifies that the address is valid, then, at step 530, **retrieves the corresponding value (the rights key) from the protected memory.** At step 550, the CryptoFirewall uses pseudoasymmetric

function F.sub.3, keyed with the rights key that was read from the protected memory at step 530, to transform the CDK generator. (In an alternate embodiment, F.sub.3 can be keyed with the CDK generator and used to transform the rights key itself. Also, F.sub.3 does not necessarily need to be a pseudoasymmetric or invertable function. For example, F3 can be a hash) At step 560, the CryptoFirewall returns the transformation result to the ICP. At step 570, the ICP optionally performs any final processing required to produce the final CDK from the F.sub.3 result. At step 580, the ICP transmits the CDK to the playback device, which, at step 590, uses the CDK to decrypt the content. [Emphasis Added]

In contrast to Kocher, a method for reproducing content stored in encrypted form on a record carrier, according to the invention, generally comprises the steps of - retrieving a carrier region code (RCC) from the record carrier, determining if the retrieved RCC matches a stored device region code (RCD), stored in the playback device, and if the match is successful, thereafter, **retrieving an encrypted region key (RK) from the record carrier** and decrypting the retrieved region key (RK) using a stored device key (DK), also stored in the playback device. Then, the decrypted RK is used to decrypt the encrypted content, stored on the record carrier.

As noted above, according to the invention, as claimed, the content decryption key is retrieved from the record carrier (see above) and not pre-stored in a protected memory, as taught in Kocher. Moreover, Kocher does not teach a multi level technique for providing a high degree against hacking, i.e., making it more difficult to make a player region code free, by first checking if a carrier region code (RCC), stored on the record carrier matches a stored device region code, and at a second level, retrieving an encrypted region key (RK) from the record carrier to be decrypted by a stored device key (RK), stored in the playback device.

Accordingly, it is believed that Applicant's Claim 1 recites patentable subject matter, and therefore, withdrawal of the rejections with respect to Claim 1 and allowance thereof is respectfully requested.

Claims 2-3 and 9-10 depend from Claim 1 and therefore include the limitations of Claim 1. Accordingly, for the same reasons given above for Claim 1, Claims 2-3 and 9-10 are believed to contain patentable subject matter. Accordingly, withdrawal of the rejections with respect to Claims 2-3 and 9-10 and allowance thereof are respectfully requested.

Independent Claims 11 and 12 recite similar subject matter as Claim 1 and therefore contain the limitations of Claim 1. Hence, for at least the same reasons given for Claim 1, Claims 11 and 12 are believed to be allowable over the cited reference. Accordingly, withdrawal of the rejection under 35 U.S.C. §102(b) and allowance of Claims 11 and 12 are respectfully requested.

Claim 13 depends from Claim 11 and therefore include the limitations of Claim 11. Accordingly, for the same reasons given above for Claim 11, Claim 13 is believed to contain patentable subject matter. Accordingly, withdrawal of the rejections with respect to Claim 11 and allowance thereof are respectfully requested.

Claims 4-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher as applied to claim 1 above, and further in view of United States Patent No. 5,907,655 to Oguro, hereinafter Oguro.

35 U.S.C. §103(a)

Claim 4-8 was rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher in view of Dierks and U.S. Patent No. 5,907,655 to Oguro.

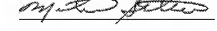
Claims 4-8 depend from Claim 1 and therefore include the limitations of Claim 1. Accordingly, for the same reasons given above for Claim 1, Claims 4-8 are believed to contain patentable subject matter. Accordingly, withdrawal of the rejections with respect to Claims 4-8 and allowance thereof are respectfully requested.

Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that all claims presently pending in the application, namely, Claims 1- 13 are believed to be in condition for allowance and patentably distinguishable over the art of record.

If the Examiner should have any questions concerning this communication or feels that an interview would be helpful, the Examiner is requested to call Mike Belk, Esq., Intellectual Property Counsel, Philips Electronics North America, at 914-945-6000.

Respectfully submitted,



Michael A. Scaturro
Reg. No. 51,356
Attorney for Applicant

Mailing Address:
Intellectual Property Counsel
Philips Electronics North America Corp.
P.O. Box 3001
345 Scarborough Road
Briarcliff Manor, New York 10510-8001